REMARKS/ARGUMENTS

Prior to entry of this amendment, the application included claims 1-65. A final Office Action mailed August 29, 2005, rejected claims 1-65 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,460,141 to Olden ("Olden").

This amendment amends claims 1, 15, 21, 26, 32, 38, 42, 46, 50, 55, 60 and 63, but neither adds nor cancels any claims. Hence, after entry of this amendment, claims 1-65 stand pending for examination.

Claim Amendments

Claim 1 has been amended to recite, "wherein said authorization services comprise determining whether said first user is authorized to access said first resource." Support for this amendment can be found throughout the specification, including at, inter alia, lines 29-30 on page 36 of the specification.

Claim 1 also has been amended to recite, "wherein authenticating said first user comprises verifying an identity of said first user." Support for this amendment can be found throughout the specification, including in particular at lines 28-29 on page 28 of the specification. Claims 15, 21, 26, 32, 38, 42, 46, 50, 55, 60 and 63 have been amended in similar fashion.

Claim 1 also has been amended to recite, "performing, at said authorization system, authorization services . . . ." Support for this amendment can be found throughout the specification, including at, inter alia, lines 1-2 on page 3 of the specification. Claims 15, 21, 26, 32, 42, 50 and 60 have been amended in similar fashion.

§ 112 Rejections

The applicant notes the withdrawal of the § 112 rejection of claim 10 and appreciates that Examiner's reconsideration of this claim.

§ 102 Rejections

All pending claims stand rejected under § 102(e) as being anticipated by Olden. These rejections are respectfully traversed, for at least the following reasons. Accordingly, reconsideration of the claims is respectfully requested.

Olden is directed to "[a] security and access management system [that] provides unified access management to address the specific problems facing the deployment of security for the Web and non-Web environment." Olden, Abstract. Pertinent to the pending claims, the system disclosed by Olden comprises "at least one authorization component 12, an entitlements (database) server component 14, an API server 16, an administrative client (graphical user interface) 18 and at least one enabled Web server 20 . . . ." *Id.*, Fig. 1 & c. 3, ll. 44-47. The authorization component 12 performs authorization processing on behalf of either an enabled Web server 20 or an API client 22." *Id.*, c. 3, ll. 52-54. Specifically, "the authorization server performs various steps for authorization, as shown in Fig. 28. In order to determine whether or not the user is valid, when an authorization server 24 receives an authentication request from either an enabled Web server 20 or from an API client 22, the authorization server performs various steps for validation, as shown in Fig. 29." *Id.*, c. 23, ll. 48-54. The entitlements database is used "for storing data utilized by the authorization server for responding to the request generated by the user to one of grant or deny the request for execution of the application by the user." *Id.*, claim 1. Hence, in the system of Olden, the authorization server performs both authentication and authorization services, while the entitlements server merely maintains the entitlements database, which holds data to be used by the authorization server.

It is respectfully submitted that the rejections of claims 1-65 evidence a misapprehension of the distinction between the authorization and authentication functions performed by an access control system. Accordingly, independent claims 1, 15, 21, 26, 32, 38, 42, 46, 50, 55, 60 and 63 have been amended to more clearly define these terms. For example, claim 1, as amended, recites, "authorization services comprise determining whether said first user is authorized to access said first resource" and "authenticating said first user comprises verifying an identity of said first user."

The method recited by claim 1 comprises, inter alia, "relying on said first authentication system for authenticating said first user" and "performing, at the authorization system, authorization services for said request to access said first resource based on said identity profile associated with said user identification information." Claim 1 also recites that "said authorization system is separate from said first authentication system." That is, in the method recited by claim 1, the authorization system and the authentication system are two separate systems, one of which (the authentication system) is responsible for verifying the identity of the user, and the other of which (the authorization system) is responsible for determining whether the user is authorized to access the requested resource.

In contrast, the authorization server of Olden performs both the authentication (determining whether the user is valid, *see* Olden, Fig. 29) and authorization (determining whether the user is authorized to access a particular URL, based on entitlements in the entitlements database, *see* Olden, Fig. 28). In other words, the authorization system of Olden does not rely on anything to perform authentication services, because the authorization system itself performs these services. This is a fundamentally different paradigm from that recited by claim 1. Indeed, the system of Olden is similar to that described in the background of the application, which notes that "products are available that authenticate and authorize users to access various content." Application, p. 2, ll. 10-11. As the application also notes, however, "there are some who want many of the services of an integrated solution, but which to continue using a legacy authentication system." *Id.*, p. 2, ll. 12-14. The method of claim 1, unlike the system described by Olden, provides the ability to use such a legacy authentication system (although it should be noted that claim 1 is not limited to the use of such legacy authentication systems).

In rejecting claims 1, the office action essentially ignores this element, failing to cite any portion of Olden that teaches or suggests relying on a separate authentication system for authenticating a user. (Similarly, the rejections of claims 15, 21, 26, 32, 38, 42, 46, 50, 55, 60 and 63 cite nothing in Olden teaching or suggesting similar elements in those claims.) Nor does a thorough review of Olden reveal any such teaching or suggestion. Instead, as noted above, in the system disclosed by Olden, the authorization server performs both authentication and

authorization services, such that the authorization server would have no need to rely on a separate authentication system to perform authentication of the user.

The office action notes that it interprets "the term 'separate' as not necessarily physical separation." The applicant does not contest this interpretation, except to note that mere "temporal separation" would appear not to teach "[an] authorization system [that] is separate from [an] authentication system" (emphasis added), as recited by claim 1.

Nonetheless, even if the term "separate" might mean "temporal separation," "virtual separation," or "software module separation," nothing in Olden teaches or suggests any separation whatsoever (however defined) between the authentication and authorization functions. A thorough review of Olden reveals only one discussion of user authentication, which can be found at column 23, lines 48-54: "[T]he authorization server performs various steps for authorization, as shown in Fig. 28. In order to determine whether or not the user is valid, when an authorization server 24 receives an authentication request from either an enabled Web server 20 or from an API client 22, the authorization server performs various steps for validation, as shown in Fig. 29." That is, Olden specifically teaches that the authorization server performs an integrated authentication/authorization process. More to the point, this discussion does not support any inference that Olden's authorization server relies on any separate authentication system to authenticate the user. In fact, the only reasonable interpretation of this passage is that Olden's authorization server performs authentication in conjunction with authorization (similar to the systems described in the background of the present application).

The office action attempts to finesse this distinction between claim 1 and Olden's system by noting that "[t]he Olden teaching of the various architectures in the architecture section . . . clearly encompasses the applicants 'separate' and 'external' network system configuration claims." The applicant does not dispute that Olden's system includes several components. Nonetheless, Olden never teaches or suggests that any of these assertedly "separate" components might perform authentication. Specifically, Olden does not teach or suggest that its authorization server (which, as noted above, performs both authentication and authorization) might comprise separate components (whether software modules or some other component) that might perform these respective functions. All Olden discloses is that a

monolithic "authorization server" performs both authentication and authorization. This does not teach or suggest the elements of claim 1.

Under § 102, "'A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.'" MPEP § 2131 (quoting *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)). As noted above, Olden fails to teach ever element of claim 1. Hence, it is believed that Olden fails to anticipate claim 1, and that the rejection of claim 1 under § 102(e) should be withdrawn. For at least similar reasons, the applicant believes that Olden fails to anticipate any of independent claims 15, 21, 26, 32, 38, 42, 46, 50, 55, 60 and 63, and that the rejections of those claims under § 102(e) should be withdrawn as well. Dependent claims 2-14, 16-20, 22-26, 28-31, 33-37, 39-46, 48, 49, 51-54, 56-59, 61, 62, 64 and 65 are believed to be allowable over Olden as depending from allowable base claim and as being directed to specific novel substitutes, and the withdrawal of the § 102(e) rejections of those claims is respectfully requested as well.

Moreover, as noted in the applicant's prior response, the use of a single system component (the authorization component) to provide both authentication and authorization services is a fundamental principle of Olden's operation. Hence, the teaching of Olden cannot be modified (or combined with another reference) to read on the pending claims without altering this fundamental principle of operation, and Olden therefore properly could not be used (either alone or in combination with other references) as the basis of a § 103 rejection of any pending claim.
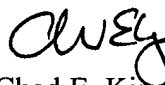
Conclusion

In view of the foregoing, Applicants believe all claims now pending in this application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.

Respectfully submitted,

Chad E. King
Reg. No. 44,187

Date: /1-29-2005

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, CA 94111-3834
Tel: 303-571-4000
Fax: 415-576-0300
CEK/jln
60616837 v1